John Mansfield, OSB No. 055390
john@harrisbricken.com
Megan Vaniman, OSB No. 124845
megan@harrisbricken.com
HARRIS BRICKEN
511 SE 11th Ave., Ste. 201
Portland, OR 97214
503-207-7313
Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

DALLAS BUYERS CLUB, LLC, Plaintiff, v. **JOHN HUSZAR,** Defendant.	Case No.: 3:15-cv-00907-AC **PLAINTIFF'S OPPOSITION TO DEFENDANT'S CROSS-MOTION FOR SUMMARY JUDGMENT**

I. INTRODUCTION

In November 2017, Plaintiff moved for summary judgment ("MSJ," Dkt. 122) on its claims that Defendant infringed its Dallas Buyers Club copyright, and that Defendant's infringement was willful. Plaintiff's MSJ relies on Defendant's admissions of liability in responses to requests for admissions, which the Court ruled are admitted after Defendant and his counsel were given many chances to answer them. Defendant's conclusive admissions "go[] beyond being mere evidence" that can be rebutted by other evidence. *Vincent v. C.O.M. House*, No. 07CV632A, 2009 U.S. Dist. LEXIS 80776, 8 (W.D.N.Y. Sept. 4, 2009). The fact finder in this case "must treat [admitted] facts as having been proved." Ninth Cir. Model Jury Instruction 2.12, Use of Requests for Admission. Despite these admissions, Defendant's opposition simply attempted to raise disputed factual issues.

Defendant's cross-motion for summary judgment ("XMSJ", Dkt. 138) is just more of the same kind of arguments he made in his opposition to Plaintiff's MSJ. First, Defendant raises a new statutory defense for system caching under the Digital Millennium Copyright Act ("DMCA") that was never pleaded or disclosed in discovery. This is precluded by Defendant's binding admissions. Even without the admissions, Defendant has not shown any facts showing that the defense is available. Second, Defendant attempts to raise a challenge to his admission that he infringed Defendant's copyright by claiming that Plaintiff must now produce a "depository copy" of the copyrighted work to prevail. This cannot rebut his admission of liability. Third, Defendant tries to raise an issue of fact as to infringement by submitting expert opinion about Plaintiff's use of evidence provided from the Maverick monitoring software. This effort also fails because of Defendant's admission of liability. Moreover, Plaintiff submits its own expert opinion about the operation of the Maverick software, which directly contradicts Defendant's expert opinions and raises disputed material facts.

II. DEFENDANT'S MOTION FOR SUMMARY JUDGMENT MUST BE DENIED.

A. Defendant cannot rely on the DMCA system caching defense of 17 U.S.C. § 512(b).

Defendant has admitted that he "copied and distributed at least portions of the motion picture *Dallas Buyers Club* through a public BitTorrent network," and that he "has used the BitTorrent protocol for the exchange of files in violation of U.S. Copyright law." RFAs 7, 5, attached as Exhibit 1 to Plaintiff's MSJ. Request for admission number 5 asks Defendant to admit the fact of copying and for the application of this fact to his liability under U.S. Copyright law. *See* Fed. R. Civ. Proc. 36(a)(1)(A). Because this Court ordered that "Plaintiff's request for admissions is deemed fully admitted based on the lack of any response by Defendant Huszar" (Dkt. No. 84), liability is admitted, Fed. R. Civ. Proc. 36(a)(3), and any objections are waived, *see id*. Defendant, who was represented by counsel when Plaintiff moved to compel responses to the RFAs, had the opportunity to respond to the RFAs in response to Plaintiff's motion, but declined to do so. Defendant may not now make objections or answer to these RFAs.

Even if a challenge were permissible despite his admissions, Defendant has not come close to making even an initial showing that the "system caching" liability limitation defense of 17 U.S.C. § 512(b) applies here. As shown in Exhibit A to this brief, Title 17, Section 512(b) is a complicated statute that contains eight numbered subdivisions (some with additional subdivisions) [1] which Defendant must prove in order to be eligible for the limitation, as made clear by the language of the statute. For example, subsection (1) of section 512(b) provides that "a service provider shall not be liable…for infringement of copyright by reason of the intermediate and temporal storage of material on a system or network controlled or operated by

[1] 17 U.S.C. §§ (b)(1)(A); (b)(1)(B); (b)(1)(C); (b)(2)(A); (b)(2)(B); (b)(2)(C); (b)(2)(D); (b)(2)(E). *See generally* Exhibit A.

or for the service provider *in a case in which,"* followed by subsections (1)(A)-(C) (emphasis added). This "preamble" requires Defendant to show facts:

- that he is a "service provider" as defined by 17 USC § 512(k)(1)(B);
- that the storage of material on the system or network was "intermediate and temporal."

Next, Defendant needs to prove that he meets subsections (1)(A)-(C), followed by the "conditions" of subsection (2)(A)-(E), including sub-subsections in (C) and (E). Defendant, however, provides *no* evidence or analysis showing that he meets any of the requirements of section 512(b)(1) or (2). Instead, Defendant makes an argument based on the following propositions: (1) anyone using a TOR router is entitled to the section 512(b) defense, and (2) Defendant was using a TOR router. Defendant has not brought forth facts supporting either premise.

First, Defendant claims that "Tor (The Onion Router) is open source software to configure their computer to serve as an 'exit point' for internet browsing for any other computer on the internet." XMSJ, p. 7. Defendant points to his counsel Edmondson's Declaration at Exhibits 4 and 5 as his sole factual support. These exhibits, however, are just two technical journal articles about TOR generally (not about Defendant's system at issue here) which Defendant appears to have proffered as "expert opinion" about how his system works. But Mr. Edmondson is not the author of either paper, and there is nothing in the record that would permit these papers to be considered as expert opinions on any question before this Court in this motion. Moreover, Defendant's brief completely fails to give any analysis based on these articles. Defendant's brief fails to "cit[e] to particular parts" of these materials as required by Fed. R. Civ. Proc. 56(c)(1)(A), or to comply with the requirement that the "party's factual positions must be

supported by citations, by page and line as appropriate, to the particular parts of materials in the record," as required by LR 56-1. *See also Simmons v. Navajo Cty., Ariz.*, 609 F.3d 1011, 1017 (9th Cir. 2010) (Courts considering summary judgment motions have "no independent duty 'to scour the record in search of a genuine issue of triable fact.'"). Even if admissible or competent, nothing in the two articles attached to Defendant's counsel's declaration shows that Defendant used a TOR router, or that any of the opinions in the articles apply to Defendant's system in this case. Nor do these articles provide any opinions that anyone using a TOR router is entitled to the section 512(b) defense.

Defendant goes on to argue that "Plaintiff has made no allegations, nor produced any evidence, that would support its claims that Huszar did anything besides run an ISP." XMSJ, p. 8. But it is not Plaintiff's burden to show that Defendant "did anything besides run an ISP." If Defendant wants to rely on the DMCA system caching defense, he must come forward with evidence showing that he has met the statutory requirements. Defendant also claims that at some unspecified portion of Defendant's deposition "there was no dispute a Tor node was used." *Id.* Defendant has again failed to provide any "citations, by page and line as appropriate, to the particular parts of materials in the record." At any rate it is difficult to imagine how a deposition of Defendant could prove "that there was no dispute a Tor node was used."

Finally, Defendant cites Judge Simon's order sanctioning Defendant (Dkt. 95) as support for his claim that "Huszar was running a Tor Service as a Service Provider," again without providing a pin cite. This finding (found on pages 7-8 of Docket 95) is simply background for Judge Simon's decision regarding Defendant's intent in overwriting hard drives. It does not find as a fact whether or not Defendant was using The Onion Router in the context of Defendant's XMSJ.

B. Defendant cannot show that there are no disputed facts that Plaintiff is not the owner of the copyright in suit.

Defendant claims that he is entitled to summary judgment that Plaintiff cannot show that it owns the copyright to *Dallas Buyers Club*. Although Defendant effectively concedes that the copyright certificate produced by Plaintiff is *prima facie* evidence that Plaintiff owns the copyright, *see, e.g., Lamp's Plus, Inc. v. Seattle Lighting Fixture Co.,* 345 F.3d. 1140, 144 (9th Cir. 2003), Defendant's conclusive admissions in this case establish that Plaintiff owns the copyright to Dallas Buyer's Club:

- [1. P]laintiff's motion picture, *Dallas Buyers Club*, contains original material that is copyrightable subject matter under the laws of the United States.
- [2. P]laintiff's motion picture, *Dallas Buyers Club*, is currently offered for sale in commerce.
- [3. P]laintiff's motion picture, *Dallas Buyers Club*, is easily discernable as a professional work as it was created using professional performers, directors, cinematographers, lighting technicians, and set designers. RFAs 1-3.

Because Defendant has admitted three times that *Dallas Buyers Club* is "Plaintiff's motion picture," he is now estopped from denying the truth of these admissions. *See International Carbonic Engineering Co. v. Natural Carbonic Products,* 57 F. Supp. 248, 253 (S.D. Cal. 1944). It follows that Defendant cannot establish that there is no disputed fact supporting his claim that Plaintiff does not own the copyright to the *Dallas Buyers Club* work.

C. Because Plaintiff does not rely on Maverick software evidence to prove infringement, admissibility of this evidence is not a material fact on which summary judgment can be granted.

Defendant's final argument is yet another effort to put forward facts to prove the opposite of what Defendant has already admitted to: he copied Plaintiff's copyrighted material in

violation of the Copyright Act. Regardless of these admissions, Plaintiff presents expert opinion that contradicts the testimony of Defendant's expert, Dr. Kal Toth, thus raising disputed material facts requiring denial of Defendant's XMSJ.

As cited in Defendant's XMSJ, Dr. Toth makes the following arguments about the MaverickMonitor software produced by the German company MaverickEye:

1. Reliability of MaverickMonitor cannot be determined absent evidence that necessary software patches were installed;
2. The size of the MaverickMonitor code base means that the number of latent defects could be large, without evidence of testing;
3. He had seen no evidence of effective testing. Defendant's XMSJ, p. 11.

Dr. Toth concludes: "In the absence of verifiable evidence, an objective software professional cannot conclude that MaverickMonitor detects the IP addresses of infringing BitTorrent users correctly, consistently and reliably." *Id.* Based on this testimony, Defendant argues that "An expert cannot 'create' reliable data from an 'unreliable' computer system," in effect arguing that such testimony would be inadmissible. *Id.* at p. 12.

As is often the case, however, there is another expert opinion in this case, which disputes Dr. Toth's opinions. Attached as Exhibit 1 to the Mansfield Declaration is the expert report of Plaintiff's expert Mr. Stephen M. Bunting. As shown by his CV and declaration paragraphs 2-14, Mr. Bunting is a highly experienced computer forensics expert with extensive experience in peer-to-peer sharing on networks.

Starting with paragraph 17 of his declaration, Mr. Bunting describes in detail his testing of the Maverick software to determine its accuracy "as to its ability to detect an infringing party's IP address, identifying metadata (client software and version used by infringer), and

identifying the known test files distributed on the torrent network." Bunting Decl., ¶ 20. Mr. Bunting tested Maverick software with four different video files, all identified by unique hash marks, with four different computers each with a different operating system. *Id.* at ¶ 22. Mr. Bunting then used Wireshark, a software tool that captures network packets (containing the files or their component pieces) transmitted over a network, to determine which files were downloaded. *Id.* at ¶ 23.

After completing several more testing steps described in paragraphs 24-29, Mr. Bunting finds:

> 30. *For all four files, the [Maverick software system] captured the public, internet-routable IP address for the source of the test or known files that I was sharing on the bit torrent network.* I knew exactly what the IP addresses were, as I had recorded them before and after the downloads. The IP addresses involved were dynamic IP addresses and thus time sensitive. The ISP's for those IP addresses maintain logs that record which subscriber or user is assigned a particular IP address at a particular time. *Had a subpoena been served on either of the two different ISP's used in this test, I would have been correctly identified as the responsible subscriber user at those exact times for those involved IP addresses*.
>
> 31. Further, *the [Maverick software system] correctly captured the exact name of the bit torrent client and version numbers that were in use by each test computer.* This capture is possible because when the [Maverick software system] connects to the computer hosting a file to be shared on the bit torrent network, a handshake occurs. Each machine's bit torrent client sends a packet to the other stating, among other things, their peer ID. Part of the peer ID is the name of the bit

torrent client followed by its version number. *Id.* at ¶¶ 30-31 (emphasis added).

Mr. Bunting also provides the following helpful explanation about how BitTorrent works and why it is so easy to determine the identity of illegal downloaders using the Maverick software:

> 44. When a user adds a torrent file for a file that they want to download, the "Trackers" that are included in the torrent file actively work to connect torrent clients that have either all or parts of a requested file with those seeking those files. In doing so, the IP addresses and port numbers, along with other metadata are shared, visible, and otherwise made public within that 'swarm' of torrent users. It is by this mechanism of identifying each computer in the swarm by its IP address and port number that computers in the swarm can connect directly to one another and share parts of the file. It is also by this mechanism that [Maverick software system] can see the public IP addresses and port numbers of copyright infringers and connect directly with them to download files and capture evidence of copyright infringement. Such a process is akin to going to a coffee shop and asking if anyone in the room has sugar on their table, as you do not. Perhaps you want 6 packets of sugar and you need a packet or two from several tables to get your 6 packets. The conversations that take place during this discovery and sharing process are very much out in the public for all in the coffee shop to hear. There is no expectation of privacy when such a request is made. Anyone in the coffee shop can see who you are and hear what it is that you are requesting. … The simple fact is that if you wish to join a peer-to-peer, file-sharing network, you have to share your IP address and port with those in that

public pool of persons doing likewise. You are agreeing to and consenting to allowing others to connect to your computer in order that you can exchange files. *As with asking for a packet of sugar in a crowded coffee shop, those in a swarm will hear your request and know who you are by your public routable IP address.* *Id.* at ¶ 44 (emphasis added).

Mr. Bunting concludes that he is "of the opinion that [the Maverick system] was designed to maintain the accuracy and integrity of the evidence throughout. *Id.* at ¶ 37. This opinion directly contradicts the opinion of Defendant's expert Dr. Toth. If this case were to go to trial, this conflict would be for the trier of fact to determine. Because there are disputed issues of material facts, Defendant's XMSJ must be denied.

III. CONCLUSION

In this case the admissibility of Defendant's admissions that he illegally copied is all that is necessary to show infringement. Because these admissions are conclusive, and for the other reasons set out above, this Court should grant Plaintiff's MSJ and deny Defendant's XMSJ.

DATED: April 9, 2018.

HARRIS BRICKEN

By: s/ John Mansfield

John Mansfield, OSB No. 055390
john@harrisbricken.com
Megan Vaniman, OSB No. 124845
megan@harrisbricken.com
511 SE 11th Ave., Ste. 201
Portland, OR 97214
503-207-7313
Attorneys for Plaintiff

EXHIBIT A: 17 U.S.C. § 512(B)

(b) System Caching.

(1) Limitation on liability. A service provider* shall not be liable for monetary relief…for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which—

(A) the material is made available online by a person other than the service provider;

(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and

(C) the storage is carried out through an automatic technical process† for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A),

if the conditions set forth in paragraph (2) are met.

(2) Conditions. The conditions referred to in paragraph (1) are that—

(A) the material described in paragraph (1) is transmitted to the subsequent users described in paragraph (1)(C) without modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A);

(B) the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available, except that this subparagraph applies only if those rules are not used by the person described in paragraph (1)(A) to prevent or unreasonably impair the intermediate storage to which this subsection applies;

(C) the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology—

(i) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material;

---

* "As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A)." 17 USC § 512(k)(1)(B).

† "A 'device,' 'machine,' or 'process' is one now known or later developed." 17 USC § 101.

(ii) is consistent with generally accepted industry standard communications protocols; and

(iii) does not extract information from the provider's system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that person;

(D) if the person described in paragraph (1)(A) has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions; and

(E) if the person described in paragraph (1)(A) makes that material available online without the authorization of the copyright owner of the material, the provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c)(3), except that this subparagraph applies only if—

(i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled; and

(ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled.